



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.   | FILING DATE | FIRST NAMED INVENTOR      | ATTORNEY DOCKET NO.           | CONFIRMATION NO. |
|---|-------------|---------------------------|-------------------------------|------------------|
| 10/723,450  | 11/26/2003  | Hung-Hsiang Jonathan Chao | CHAO 1-77-1-14<br>(LCNT/1260) | 5965             |
| 46363   | 7590        | 04/23/2008                | EXAMINER                      |                  |
| PATTERSON & SHERIDAN, LLP/<br>LUCENT TECHNOLOGIES, INC<br>595 SHREWSBURY AVENUE<br>SHREWSBURY, NJ 07702 |             |                           | KANE, CORDELIA P              |                  |
|   |             |                           | ART UNIT                      | PAPER NUMBER     |
|   |             |                           | 2132                          |                  |
|   |             |                           | MAIL DATE                     | DELIVERY MODE    |
|   |             |                           | 04/23/2008                    | PAPER            |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                      |   |  |
|------------------------------|--------------------------------------|---|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>10/723,450 | <b>Applicant(s)</b><br>JONATHAN CHAO ET AL. |  |
|                              | <b>Examiner</b><br>CORDELIA KANE     | <b>Art Unit</b><br>2132                     |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 20 February 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12, 15, 18-21, 23 and 25-28 is/are rejected.
- 7) ☒ Claim(s) 13, 14, 16, 17, 22 and 24 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments filed February 20, 2008 have been fully considered but they are not persuasive. Applicant argues that Chesla fails to teach plurality of security perimeter routers. However, Chesla clearly depicts and states that there are a plurality of routers located at the periphery of the network (figure 1C, and page 7, paragraph 118). These routers work with the network appliance and therefor are part of the security system. Chesla teaches a plurality of security perimeter routers.

2. Applicant goes on to argue that Lau fails to teach the plurality of security perimeter routers. However, Lau teaches that there is a router and network processor located on the perimeter of the network (Figure 1) and goes on to teach that there could be a plurality of network processors (page 2, paragraph 16). Therefor they form a plurality of security perimeter routers.

### ***Claim Rejections - 35 USC § 102***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 3, 8 – 12, 15, 18 – 21, 23, and 25 – 28 are rejected under 35 U.S.C. 102(e) as being anticipated by Chesla et al's US Publication 2004/0250124 A1. Referring to claim 1, Chesla teaches:

- a. Confirming a DDoS attack at a network location using a plurality of packet attribute values (page 23, paragraph 376) aggregated from a plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118).
  - b. Computing an aggregate conditional probability measure for each packet entering said location based on a selected attributes included within said packets (page 14, paragraph 224).
  - c. Computing an aggregate cumulative distribution function of scores based on said computed aggregate conditional probability function (page 14, paragraph 225).
  - d. Determining a discarding threshold using said cumulative probability function (page 14, paragraph 225).
  - e. Sending said discarding threshold to each of the routers (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.
5. Referring to claim 3, Chesla teaches granting immunity to packets of a specified sub-type entering said location (page 13, paragraph 199).
6. Referring to claim 8, Chesla teaches:
  - f. Aggregating victim destination prefix lists and attack statistics associated with incoming packets received (page 14, paragraph 224) from said plurality of routers forming a security perimeter (Figure 1C, page 7, paragraph 118) to confirm a DDoS attack (page 23, paragraph 376). Since each potential victim

would have the same prefix since it is on the same customer network, the aggregating of the statistics would also be an aggregation of the victim prefix list.

g. Aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers (page 14, paragraph 224).

h. Generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles (page 14, paragraph 225).

i. Providing to each of the router a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.

7. Referring to claim 9, Chesla teaches comparing measured attribute values with nominal attribute values, and identifying increases in said measured attribute values over said nominal values (page 9, paragraph 137).

8. Referring to claim 10, Chesla teaches determining if said increase for said measured attribute value exceeds respective predetermined thresholds (page 9, paragraph 137).

9. Referring to claim 11, Chesla teaches that attack statistics includes flow counts (page 3, paragraph 33).

10. Referring to claim 12, Chesla teaches receiving packet attribute distribution frequencies including incoming packet attribute information comprising at least TTL (page 4, paragraph 45).

11. Referring to claim 15, Chesla teaches computing a partial score of different attributes and computing a weighted sum of the partial scores to yield a logarithmic function of conditional legitimate probability (page 15, paragraph 236).

12. Referring to claims 18 and 28, Chesla teaches:

j. Sending from each of the plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118) victim destination prefix list and attack statistics associated with incoming packets to a centralized controller adapted to confirm a victim of DDoS attack (page 20, paragraph 322-323).

k. Sending, from each of the plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118), packet attribute distribution frequencies for incoming victim related packets (page 16, paragraph 243).

l. Receiving at each of the plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118) from said centralized controller common scorebooks formed by aggregated packet attribute distribution frequencies (page 14, paragraph 225).

m. Sending from each of the plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118) local cumulative distribution function of scores to said centralized controller (page 13, paragraph 212).

- n. Discarding at each of the plurality (Figure 1C) of security perimeter routers (page 7, paragraph 118) incoming packets based on a commonly distributed discarding threshold defined by said centralized controller (page 23, paragraph 372)
- 13. Referring to claim 19, Chesla teaches classifying packets as suspicious or non-suspicious (page 17, paragraph 264) based on the destination address of the packet (page 17, paragraph 278).
- 14. Referring to claim 20, Chesla teaches that attack statistics includes flow counts (page 3, paragraph 33).
- 15. Referring to claim 21, Chesla teaches receiving packet attribute distribution frequencies including incoming packet attribute information comprising at least TTL (page 4, paragraph 45).
- 16. Referring to claim 23, Chesla teaches:
  - o. Determining a predetermined number of packets to monitor (page 16, paragraph 247).
  - p. For each incoming packet: determining attribute scores and locally aggregating said scores (page 16, paragraph 247).
  - q. Forming said CDF from said aggregated scores associated with the predetermined number of incoming packets (page 16, paragraph 249).
- 17. Referring to claim 25, Chesla teaches:
  - r. Determining whether a score of an incoming packet is less than or equal to said discarding threshold, discarding said incoming packet if said score is less

than or equal to said threshold, and forwarding the incoming packet if said score is greater than the threshold (page 11, paragraph 173).

18. Referring to claim 26, Chesla teaches:

s. Means for aggregating a plurality of packet attribute values respectively received from a plurality of routers forming a security perimeter on the network (Figure 1C, page 7, paragraph 118) to confirm said attack at said location (page 23, paragraph 376), wherein the controller is associated with the network (Figure 1C).

t. Means for computing an aggregate conditional probability measure for each packet entering said location based on selected attributes included within said packet from each location (page 14, paragraph 224).

u. Means for computing an aggregate cumulative distribution function (CDF) based on said computed aggregate conditional probability measures (page 14, paragraph 225).

v. Means for determining a drop threshold based on access to said cumulative probability function (page 14, paragraph 225).

w. Means for sending said drop threshold to each of said routers, (page 20, paragraph 323) wherein said routers are adapted to pass through packets that exceed said determined drop threshold to said location (page 20, paragraph 322).

19. Referring to claim 27, Chesla teaches:

- x. Means for aggregating, local victim destination prefix lists and attack statistics associated with incoming packets received from a plurality of routers (page 14, paragraph 224) forming a security perimeter in said network to confirm a victim of said DDoS attack (page 23, paragraph 376) wherein the centralized controller is associated with the network (Figure 1C). Since each potential victim would have the same prefix since it is on the same customer network, the aggregating of the statistics would also be an aggregation of the victim prefix list.
- y. Means for aggregating packet attribute distribution frequencies for incoming victim related packets received from said plurality of security perimeter routers (page 14, paragraph 224).
- z. Means for generating common scorebooks from said aggregated packet attribute distribution frequencies and nominal traffic profiles (page 14, paragraph 225).
- aa. Means for aggregating local cumulative distribution function (CDF) of the local scores derived from said plurality of security perimeter routers (page 13, paragraph 212).
- bb. Means for providing, to each of said plurality of security perimeter routers, a common discarding threshold, said discarding threshold defining a condition in which an incoming packet may be discarded at said security perimeter (page 20, paragraph 323). Since the filtering would be in the routers then the information computed in the FIS module would have to be passed to the filters/routers, to be able to filter.

20. Claims 1 – 7 and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Lau et al's US Publication 2004/0062199 A1.

21. The applied reference has a common inventor and assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

22. Referring to claim 1, Lau teaches:

cc. Confirming a DDoS attack at a network location using a plurality of packet attribute values aggregated from said plurality of security perimeter (page 2, paragraph 16) routers (page 1, paragraphs 4 and 14).

dd. Computing an aggregate conditional probability measure for each packet entering said location based on a selected attributes included within said packets (page 3, paragraph 41).

ee. Computing an aggregate cumulative distribution function of scores based on said computed aggregate conditional probability function (page 3, paragraph 41).

ff. Determining a discarding threshold using said cumulative probability function (page 2, paragraph 31).

- gg. Sending said discarding threshold to each of the routers (page 2, paragraph 16). Since there may be multiple routers or NPs then the information would need to be distributed.
23. Referring to claim 2, Lau teaches updating an individual marginal probability mass function and a join probability mass function (page 3, paragraph 41).
24. Referring to claim 3, Lau teaches granting immunity to packets of a specified sub-type entering said location (page 2, paragraph 31).
25. Referring to claim 4, Lau teaches the equation:  $CP(p) = \frac{n}{m} * \frac{JP_n}{JP_m} (A = a_p, B = b_p, C = c_p, ) / (A = a_p, B = b_p, C = c_p, )$  (page 2, equation 1).
26. Referring to claim 5, Lau teaches the equation:  $CP(p) = \frac{n}{m} * \frac{P_n(A=a_p)}{P_m(A=a_p)} * \frac{P_n(B=b_p)}{P_m(B=b_p)} * \frac{P_n(C=c_p)}{P_m(C=c_p)}$  (page 2, equation 2).
27. Referring to claim 6, Lau teaches that the discarding threshold is calculated using a load shedding algorithm, combined with an inverse lookup on the aggregate CDF of scores (pages 4-6, paragraph 61).
28. Referring to claim 7, Lau teaches that said joint and marginal probability functions are maintained using iceberg-style histograms (page 4, paragraph 46).
29. Referring to claim 26, Lau teaches all the limitations that are equivalent to claim 1, and passing through packets that exceed said determined drop threshold to said location (page 1, paragraph 7).

***Allowable Subject Matter***

30. Claims 13, 14, 16, 17, and 22, and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

31. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. K./  
Patent Examiner, Art Unit 2132

/Gilberto Barron Jr/  
Supervisory Patent Examiner, Art Unit 2132